Department of Homeland Security Daily Open Source Infrastructure Report for 05 April 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Houston Chronicle reports two federal air marshals pleaded guilty on Tuesday, April 4, to drug and bribery charges and agreed to cooperate with prosecutors, raising the possibility that other air marshals are under investigation. (See item 21)
- The Los Alamos National Laboratory reports that using supercomputers to respond to a potential national health emergency, scientists have developed a simulation model that makes predictions about the possible future course of an avian influenza pandemic. (See item 39)
- Emergency managers at all levels of government plan to attend the 28th Annual National Hurricane Conference in Orlando, April 10−14, reflecting intense concerns about hurricane threats that have swept the nation in recent years. (See item 41)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 04, Reuters* — **Calpine to sell about a fifth of its plants.** Calpine Corp. said it plans to sell about a fifth of its power plants in a bid to reemerge from bankruptcy as a leaner company centered around its profitable operations. Calpine said it will keep a portfolio of geothermal and gas−fired power plants in key markets after the asset disposals. The company plans to sell about

20 plants in undisclosed locations that it no longer considers to be core operations.
Source: http://biz.yahoo.com/rb/060404/utilities_calpine.html?.v=2

2. *April 04, Associated Press* — **EU pushes governments to open up gas and electricity markets.** European Union (EU) regulators on Tuesday, April 4, started legal proceedings against 17 countries for not doing enough to open up their energy markets. Delays in drafting new rules to liberalize gas and electricity markets are keeping prices too high, the European Commission has said. Austria, Belgium, Britain, the Czech Republic, Germany, Estonia, Spain, Finland, France, Greece, Ireland, Italy, Lithuania, Latvia, Poland, Sweden, and Slovakia will all be sent a second warning to put rules in place. Spain will be warned for not applying them properly. The EU criticized the lack of free choice of supplier for many customers and the continued existence of regulated prices, saying that made it harder for new companies to break into the energy sector. High oil prices and a gas dispute between Russia and Ukraine this winter have made energy a sore point for some governments anxious to protect old monopolies from foreign predators wanting to take advantage of a move toward a single European energy market. Only five countries had adopted rules opening up the gas and electricity markets for business customers by July 1, 2004.
Source: http://biz.yahoo.com/ap/060404/eu_energy.html?.v=3

3. *April 04, Government Accountability Office* — **GAO−06−555T: Plants Have Upgraded Security, but the Nuclear Regulatory Commission Needs to Improve Its Process for Revising the Design Basis Threat (Testimony).** The nation’s commercial nuclear power plants are potential targets for terrorists seeking to cause the release of radioactive material. In April 2003, in response to the terrorist attacks of September 11, 2001, the Nuclear Regulatory Commission (NRC) revised the design basis threat (DBT), which describes the threat that plants must be prepared to defend against in terms of the number of attackers and their training, weapons, and tactics. NRC also restructured its program for testing security at the plants through force−on−force inspections (mock terrorist attacks). This testimony addresses the process NRC used to develop the April 2003 DBT for nuclear power plants, the actions nuclear power plants have taken to enhance security in response to the revised DBT, and NRC’s efforts to strengthen the conduct of its force−on−force inspections. This testimony is based on the Government Accountability Office's (GAO) report on security at nuclear power plants, issued on March 14, 2006 (GAO−06−388). In its March 2006 report, GAO recommended that NRC improve its process for making changes to the DBT and evaluate and implement measures to further strengthen its force−on−force inspection program.
Highlights: http://www.gao.gov/highlights/d06555thigh.pdf
Source: http://www.gao.gov/docsearch/repandtest.html

4. *April 04, Associated Press* — **Demand may outpace Saudi oil capacity.** Demand for oil is rising so fast that even Saudi Arabia's vast resources will be unable to cope without drastic help, oil executives and analysts say. Remarkably, even Saudis, who control over a quarter of the world's known oil, are calling for relief from relentless consumption. Ghazi Al−Rawi, head of private equity at Gulf One Investment Bank, said "The current out−of−control demand is not good for us...When you have this kind of demand, you're forced to supply beyond the optimal rate." Most urgently needed is energy conservation, especially in the United States, which now burns up a quarter of the oil sold to the world, said Saddad al−Husseini, the former head of production at state−owned Saudi Aramco. Also critical is the development of fuels from

oil−rich sands or natural gas that can act as substitutes for oil. Other producing countries, such as Iran and Iraq, could ease the crunch by boosting exports to handle a greater share of the surging demand in China and India. If such help doesn't materialize and Saudi Arabia maxes its output, the kingdom's proven reserves might only sustain those gushing flows for a couple of decades before starting to dwindle, al−Husseini said.
Source: http://news.yahoo.com/s/ap/20060403/ap_on_bi_ge/saudi_more_o il_bizspotlight_1

5. *April 03, Agence France−Presse* — **Merkel announces massive investment in German energy research.** German Chancellor Angela Merkel said the country's big energy companies had pledged billions of dollars of investment in infrastructure, new plants, and renewable energy sources by 2012 to help Germany reshape its energy policy. Merkel hopes the new energy policy will make Germany less reliant on foreign suppliers. Merkel's stated aim is to draft a new energy policy by the end of next year that will map out Germany's approach until 2020. Economy Minister Michael Glos and Environment Minister Sigmar Gabriel said that heavy reliance on mineral oil meant that Germany and the European Union would remain dependent on "politically unstable supply regions." Merkel said Germany has pledged to phase out nuclear energy by 2020.
Source: http://www.turkishpress.com/news.asp?id=116936

6. *April 03, Associated Press* — **Failed attack boosts Saudi security image.** When al Qaeda−linked extremists attacked the giant Abqaiq oil processing plant near Dammam in February, many security analysts said the attack heralded a new risk to secure exports of the kingdom's oil, and the price of crude jumped quickly. Three weeks later, oil analysts say the failed car bombs did more to assure investors of the strength of Saudi Arabia's security precautions than they did harm. The $2−a−barrel hike in the oil price evaporated once it became clear the attack had failed, said Sharif Ghalib of Energy Intelligence Research. Ghalib and others said the failure of what appeared to be a well−planned attack by militants driving trucks labeled with the Saudi oil company logo has validated Saudi Arabia's investments in security infrastructure and redundant export and storage systems. The kingdom plans to spend $2 billion of its $12 billion 2006 defense budget to protect the country's oil sector, said Nawaf Obaid, a Saudi petroleum adviser. Riyadh has also started discussing the creation of special oil−sector troops and an intelligence agency focusing on threats to the energy industry, Obaid said. U.S. Navy warships form one part of a multilayered force protecting Saudi Arabia's Gulf export terminals, he said.
Source: http://seattlepi.nwsource.com/business/1310AP_Saudi_Oil_Secu rity.html

7. *April 03, Associated Press* — **Chavez tightens grip on energy resources.** President Hugo Chavez has tightened his grip on Venezuela's energy resources, following through on threats to punish international companies that resist government control of the nation's oil fields. Venezuela seized two oil fields from France's Total SA and Italy's Eni SpA after the companies failed to comply with a government demand that operations be turned over to state oil company Petroleos de Venezuela SA, or PDVSA, Oil Minister Rafael Ramirez said Monday, April 3. Ramirez, asked if companies that resist will be forced out of Venezuela, replied: "We don't have a veto against any company here." But he added: "Companies that don't adjust to our laws, we don't want them to continue in the country." Until PDVSA took control of the oil fields Saturday, Total and Eni had operated them under contract. Some other companies, including Exxon Mobil Corp., decided to sell their stakes among the 32 Venezuelan oil properties rather

than go along with the new terms. Venezuela's weekend seizures were the first as part of Chavez's effort to draw more revenue from companies pumping crude in the South American country.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/03/AR2006040300736.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

8. *April 04, KXAS (TX)* — **Chemical spill shut down Texas interstate.** Both directions of Interstate−20 in Fort Worth, TX, were closed after a chemical spill involving a tractor−trailer carrying a non−flammable chemical. About 1,000 gallons of oil lubricant spilled into both lanes.
Source: http://www.msnbc.msn.com/id/12149025/from/RSS/

9. *April 04, KTUL (OK)* — **Tanker truck explodes, prompts turnpike closure.** At least four people were injured early Tuesday morning, April 4, after a tanker truck caught fire and exploded on the Will Rogers Turnpike near Big Cabin, OK. Both the eastbound and westbound lanes of the turnpike were shut down.
Source: http://www2.ktul.com/news/stories/0406/316258.html

[Return to top]

Defense Industrial Base Sector

10. *April 04, Aviation Now* — **Congressional study looks at long−range strike alternatives.** The Department of Defense's long−range strike project would get more bang for its buck using missile−firing large cargo aircraft, like the C−17, but their vulnerability to enemy air defenses would severely limit their offensive reach, according to a study by the Congressional Budget Office (CBO). The 75−page report, prepared before the release of the 2006 Quadrennial Defense Review, examines several alternatives for developing a long−range strike system. The CBO cautioned against an all−or−nothing approach, however. Depending on the specific requirements the Pentagon determines are needed, "the preferred solution might include more than one of the systems CBO examined," stated the report.
CBO's study: http://www.cbo.gov/ftpdocs/71xx/doc7112/03−31−StrikeForce.pd f
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/LONG04046.xml

11. *April 04, Government Accountability Office* — **GAO−06−564T: Defense Acquisitions: Improved Business Case Key for Future Combat System's Success (Testimony).** The Future Combat System (FCS) is a networked family of weapons and other systems in the forefront of efforts by the Army to become a lighter, more agile, and more capable combat force. When considering complementary programs, projected investment costs for FCS are estimated to be on the order of $200 billion. FCS’s cost is of concern given that developing and producing new weapon systems is among the largest investments the government makes, and

FCS adds significantly to that total. Over the last five years, the Department of Defense (DoD) doubled its planned investments in such systems from $700 billion in 2001 to $1.4 trillion in 2006. At the same time, research and development costs on new weapons continue to grow on the order of 30 to 40 percent. FCS will be competing for significant funds at a time when federal fiscal imbalances are exerting great pressures on discretionary spending. In the absence of more money being available, FCS and other programs must be executable within projected resources. This testimony discusses (1) the business case needed for FCS to be successful and (2) the Government Accountability Office's recent recommendations to DoD and matters for congressional consideration regarding the FCS program.
Highlights: http://www.gao.gov/highlights/d06564thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−564T

12. *April 04, Government Accountability Office* — **GAO−06−548T: Force Structure: Capabilities and Cost of Army Modular Force Remain Uncertain (Testimony).** The Army considers its modular force transformation the most extensive restructuring it has undertaken since World War II. Restructuring the Army from a division−based force to a modular brigade−based force will require extensive investments in equipment and retraining of personnel. The foundation of the modular force is the creation of standardized modular combat brigades designed to be stand−alone, self−sufficient units that are more rapidly deployable and better able to conduct joint operations than their larger division−based predecessors. The Government Accountability Office (GAO) was asked to testify on the status of the Army's modularity effort. This testimony addresses (1) the Army's cost estimate for restructuring to a modular force, (2) progress and plans for equipping modular combat brigades, (3) progress made and challenges to meeting personnel requirements, and (4) the extent to which the Army has developed an approach for assessing modularity results and the need for further adjusting designs or implementation plans. This testimony is based on previous and ongoing GAO work examining Army modularity plans and cost. GAO has suggested that Congress consider requiring the Secretary of Defense to provide a plan for overseeing spending of funds for modularity.
Highlights: http://www.gao.gov/highlights/d06548thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−548T

13. *April 03, Government Accountability Office* — **GAO−06−284: Contract Security Guards: Army's Guard Program Requires Greater Oversight and Reassessment of Acquisition Approach (Report).** Following the terrorist attacks of September 11, 2001, increased security requirements and a significant number of active duty and reserve personnel sent overseas to support the war on terror left the Department of Defense (DoD) with fewer military personnel to rely on to protect domestic installations. To correct this shortage, Congress is temporarily allowing DoD to use contract security guards to fulfill roles previously performed by military employees. The U.S. Army has awarded contracts worth nearly $733 million to acquire contract guards at 57 Army installations, an investment far greater than those made by other DoD services so far. The requesters asked the Government Accountability Office (GAO) to assess how the Army has been managing and overseeing its acquisition of security guard services, particularly with regard to the Army's (1) acquisition strategy, (2) employment screening, (3) training of contract guards, and (4) award fee process. GAO made recommendations to the Secretary of Defense to improve management and oversight of the contract security guard program. In written comments on a draft of this report, DoD agreed with the recommendations

and stated that the Department of Army is implementing them.
Highlights: http://www.gao.gov/highlights/d06284high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−284

[Return to top]

Banking and Finance Sector

14. *April 04, Security Park* — **Cyber criminals are no longer limiting themselves to attacking individuals.** Cybercriminals are starting to target mobile devices such as smartphones, but smartphone adoption will need to reach a critical mass before cybercriminals actively target them as source for financial gain, according to a report by Kaspersky Lab. In addition, the report highlights the shift away from individuals being targets of malicious attacks and the trend towards the increasing attacks against government organizations. The report examines the evolution of the criminal underground and provides an overview of the criminalization of the Internet during 2005. The report discusses the escalating confrontation between cybercriminals and the anti−virus industry, the speed of response to new threats, social engineering techniques, technologies used to increase profit through cybercrime, and recommendations for users. One of the strongest trends in 2005 was the escalation of confrontation, both between cybercriminals and the antivirus industry, but also among cybercriminals themselves. In 2005, cybercriminals stepped up their attacks against governmental organizations; this indicates that they are no longer satisfied with the profits made from individual users.
Malware Evolution 2005, part II
report:http://www.viruslist.com/en/analysis?pubid=182974451.
Source: http://www.securitypark.co.uk/article.asp?articleid=25171&Ca tegoryID=1

15. *April 03, Websense Security Labs* — **Phishing Alert: Financial Partners Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Financial Partners Credit Union. Users receive a spoofed e−mail that claims that their account information needs to be verified. The spoofed e−mail instructs the user to confirm account information by following a link to a phishing Website. Users who visit this Website are prompted to enter their account password and credit card information.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =453

16. *April 03, Websense Security Labs* — **Phishing Alert: San Diego County Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of San Diego County Credit Union. Users receive a spoofed e−mail that claims that specified services will be terminated if the services are not updated. The message provides a link to a phishing Website to update the account. Users who visit this Website are prompted to enter their account number and password.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =454

17. *April 03, CNET News* — **Payment processor fears credit card crooks.** A major online payment provider said Monday, April 3, that its processing service had been used in an attempt to charge money to stolen credit and debit cards. Several Web hosting companies that use the Authorize.Net service to accept credit cards online saw a sudden spike in transactions over the

weekend. The transactions, most for $500 and $700, were billed to Visa, MasterCard, and American Express cards that belong to people across the U.S., representatives for three Web hosts said. "These hackers got their hands on high quality data, and they used merchants of ours to run that data through the merchant's Website, which goes through our platform," said David Schwartz, a spokesperson for Authorize.Net. The company says more than 130,000 merchants use its online payment service. The Web hosting companies discovered the unusual charges through e−mail alerts that Authorize.Net sends after each transaction. Close to 3,000 suspicious transactions were pushed through the merchant accounts of three companies with which CNET News.com spoke, and more likely happened at other Web hosts, these three companies said.
Source: http://news.com.com/Countless+dens+of+uncatchable+thieves/2100−1029_3−6056884.html?tag=cd.top

18. *April 03, BusinessWeek* — **Scammers find new ways to trick people −− not technology −− to get information.** As Web−based scams proliferate, it's often psychological cunning, deployed on top of surreptitious code that is the secret to cyber criminals' success. Internet scammers need a never−ending supply of ways to convince victims to trust them −− to open an attachment or click a link. Hackers are spending serious effort in researching the psychological vulnerabilities of potential targets. David Perry of TrendMicro says scammers watch news headlines for poignant world events and review the success of an attack by reading press releases, in order to tweak the next attack for greater effectiveness. Hackers also look for situations of confusion to exploit, such as a corporate merger. Once they used a bogus e−mail from someone pretending to be a helpdesk employee trying to verify account data for a database that was being combined after a merger. Analysts say phishing attacks also often spike after a data security breach hits news headlines because customers are already anticipating a potential request to update account data and monitor credit reports. Law enforcement agents say cyber−criminals pool their brainpower to devise new techniques. A DVD available in foreign black markets called "Hacker's Handbook" contains tips on how to trick victims, according to Trend Micro's Perry.
Source: http://www.businessweek.com/technology/content/apr2006/tc20060403_673342.htm?chan=technology_technology+index+page_today

19. *April 03, CSO Online* — **Secret Service closes investigation of missing tapes.** The U.S. Secret Service has closed three high−profile investigations involving backup tapes from Bank of America Corp., Citigroup Inc., and Time Warner Inc. that were reported lost in transit to storage facilities in 2005. The tapes contained personal data on hundreds of thousands of consumers. Dale Pupillo of the Secret Service said, "Although we can't prove what happened, we suspect that the tapes were lost or disposed of in the normal course of transportation. They were damaged or discarded. We don't suspect anyone of having deliberately stolen the tapes." The rash of tapes that have gone missing have spurred businesses and the federal government to strengthen their security procedures. Iron Mountain Inc. now offers customers an "extended level of protection for high−value tapes" that includes special processing instructions for an additional fee. Congress is also looking at several bills to protect personal data, including one requiring companies to notify police, consumers and credit card issuers of a breach. The Secret Service is using its Electronic Crimes Task Force meetings to offer guidance.
Source: http://www.computerworld.com/hardwaretopics/storage/story/0,10801,110170,00.html

20.

April 03, Reuters — **China warns banks against counterfeit U.S. notes.** China's central bank has warned lenders to be on guard against counterfeit US$100 notes, in a move that could signal the latest irritant in the relationship between North Korea and Beijing, its most important ally. The statement from the People's Bank of China did not specify the origin of the fake bills, but said they came from outside China and referred to them as "supernotes" −− the word the U.S. government uses for the high−quality counterfeit money it says is printed by North Korea. "These fake American notes have flowed from outside across our borders. Criminals attempt to use them for money laundering activities through smuggling and trafficking," said the notice on the central bank's Website. The United States has been getting tough on firms it suspects of aiding Pyongyang's illegal financial activities. The criminal sector may account for 35 to 40 percent of North Korea's export earnings, scholar David Asher said in a report published by the Nautilus Institute think−tank. Others have estimated it earns tens of millions a year through illegal means and analysts say Pyongyang avoids legitimate economic activity out of fears it will lead to political change.
Source: http://news.yahoo.com/s/nm/20060403/us_nm/china_korea_counte rfeit_dc_1

[Return to top]

Transportation and Border Security Sector

21. *April 04, Houston Chronicle* — **Air marshals plead guilty in drug, bribery case.** Two federal air marshals pleaded guilty on Tuesday, April 4, to drug and bribery charges and agreed to cooperate with prosecutors, raising the possibility that other air marshals are under investigation. Burlie L. Sholar III, 38, and Shawn Ray Nguyen, 32, pleaded guilty to agreeing to accept $15,000 in return for using their positions as air marshals to bypass security to smuggle 15 pounds of cocaine on a flight to Las Vegas. Their arrests raised concerns about airport security, with prosecutors pointing out during a detention hearing in February that Nguyen had smuggled other items in a briefcase and had stated that he didn't care what the briefcase contained. In their plea agreements, the two admit that they discussed accepting $5,000 per kilogram from an FBI informant in exchange for trying to smuggle 15 kilograms, or about 33 pounds, of cocaine past security at Bush Intercontinental Airport and onto a flight bound for Las Vegas. Assistant U.S. Attorney Mark McIntyre said the investigation was continuing, but cautioned against the expectation of more arrests.
Source: http://www.chron.com/disp/story.mpl/metropolitan/3767442.htm l

22. *April 04, Associated Press* — **Delta pilots vote to authorize strike.** Delta Air Lines pilots, angered by management's effort to throw out their contract and impose deep pay cuts, on Tuesday, April 4, voted by a wide margin to authorize a strike, union leaders said. The 94.7 percent vote in favor of authorizing a strike gives union leaders the authority to set a strike date. The nation's third largest carrier, which is operating under bankruptcy protection, has said a strike would put it out of business.
Source: http://www.usatoday.com/travel/flights/2006−04−04−delta−vote_x.htm

23. *April 04, Baltimore Sun* — **MARC rush hour adds security.** Beginning on Tuesday, April 4, and going until April 28, all rush−hour riders at the MARC commuter rail station in Dorsey, MD, will have to walk through a 20−foot−long box to be scanned for explosives, part of a test of a mobile screening device that eventually could be deployed nationwide. The mobile

checkpoint uses technology found at the nation's airports since the terrorist attacks of September 11, 2001, and puts it in two standard shipping containers that sit side by side. They can be moved from station to station on a flatbed truck within a day. Security on mass transit, particularly commuter rail and bus lines, has been tricky for Transportation Security Administration to manage. The primary threats to trains and buses are from bombs carried aboard, as in terror attacks on transit systems in London, Madrid, and Moscow. But screening millions of people every day at every station across the country would likely be cost−prohibitive and slow commutes to a crawl. Security experts say transit officials might have to settle for a system deployed only during a crisis or as a random deterrent. Transit authorities now primarily rely on bomb−sniffing dogs, video surveillance, random searches of riders and their bags, and tips from riders and employees.
Source: http://www.baltimoresun.com/business/bal−bz.tsa04apr04,0,6463861.story?coll=bal−business−headlines

24. *April 04, Department of Transportation* — **DOT looking for universities to tackle nation's transportation challenges.** The Department of Transportation (DOT) is inviting colleges and universities across the country to compete over the next two months to receive approximately $6 million in federal transportation research funds. The ten winning schools will be designated as Regional University Transportation Centers (UTC) for a three−year period. Applications for the merit−based competition are due by June 1, and the Department will make its selections by July 14. Once selected, the new UTCs will be expected to provide leadership in solving national and regional transportation problems facing the nation today, Secretary of Transportation Norman Y. Mineta said. The 10 current UTCs are the Massachusetts Institute of Technology, the City College of New York, the Pennsylvania State University, the University of Tennessee, the University of Wisconsin−Madison, Texas A&M University, Iowa State University, North Dakota State University, the University of California, and the University of Washington. The UTC program is administered by DOT's Research and Innovative Technology Administration. Application forms and instructions can be accessed online at http://utc.dot.gov or http://www.grants.gov
Source: http://www.dot.gov/affairs/rita0206.htm

25. *April 04, Government Accountability Office* — **GAO−06−542T: Border Security: Reassessment of Consular Resource Requirements Could Help Address Visa Delays (Testimony).** In deciding to approve or deny a visa application, the Department of State's (State) consular officers are on the front line of defense in protecting the United States against those who seek to harm U.S. interests. To increase border security following the September 11 attacks, Congress, State, and the Department of Homeland Security initiated a series of changes to border security policies and procedures. These changes have added to the complexity of consular workload. But consular officers must balance this security responsibility against the need to facilitate legitimate travel. In recent years, the Government Accountability Office (GAO) has issued a series of reports on the visa process. This statement discusses (1) wait times for visas, (2) factors that affect wait times, and (3) GAO's recent work on consular staffing. We recommended in October 2002 and again in September 2005 that State reassess its consular staffing requirements. In commenting on a draft of GAO's September 2005 report, State disagreed with our recommendation that it prepare a plan to address consular requirements. In light of the increased workload due to additional border security requirements and ongoing staffing shortages and processing delays at some posts, GAO continues to urge State to fully

assess its resource needs to ensure it has the right people at key posts.
Highlights: http://www.gao.gov/highlights/d06542thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−542T

26. *April 04, Government Accountability Office* — **GAO−06−572T: Highway Trust Fund: Overview of Highway Trust Fund Estimates (Testimony).** The Highway Trust Fund is the principal mechanism for funding federal highway and transit programs through receipts from excise taxes charged to highway users, such as taxes on motor fuels. The Department of Treasury (Treasury) and the Congressional Budget Office (CBO) each prepare estimates of future receipts for the Highway Trust Fund semiannually. Treasury's receipt estimates are combined with the Department of Transportation's estimates of outlays to create an estimate of the Highway Trust Fund balance for the President's Budget; CBO also projects outlays to develop an estimate of the fund balance. The agencies' most recent estimates show that the Highway Account within the Highway Trust Fund could have a negative balance as early as 2009, raising concerns about whether funding for federal highway programs—which were recently authorized by the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users—will continue to be met. Consequently, the Subcommittee asked us to review and compare recent estimates made by Treasury and CBO. This testimony provides information on how (1) estimates are used to provide key information about the Highway Trust Fund, (2) the most recent Highway Trust Fund estimates—based on receipt estimates made by Treasury and CBO—compare, and (3) Treasury's and CBO's estimates compare to actual receipts for recent years.
Highlights: http://www.gao.gov/highlights/d06572thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−572T

27. *April 04, Government Accountability Office* — **GAO−06−371T: Aviation Security: Enhancements Made in Passenger and Checked Baggage Screening, but Challenges Remain (Testimony).** Securing commercial aviation is a daunting task—with hundreds of airports, thousands of aircraft, and thousands of flights daily carrying millions of passengers and pieces of checked baggage. It has been over 3 years since the Transportation Security Administration (TSA) assumed responsibility for passenger and baggage screening at commercial airports. This testimony focuses on the progress TSA is making in strengthening airline passenger and checked baggage screening and the challenges that remain. Particularly, this testimony highlights TSA's efforts to (1) enhance the performance, management, and deployment of the transportation security officer workforce; (2) strengthen procedures for screening passengers and checked baggage; and (3) leverage and deploy screening technologies. In prior reports, the Government Accountability Office (GAO) has made numerous recommendations designed to strengthen aviation security, to include passenger and checked baggage screening operations. TSA generally agreed with our recommendations and is taking actions to implement them. GAO also has several ongoing reviews related to the issues addressed in this testimony, and will issue separate reports related to these areas at later dates, with additional recommendations as appropriate.
Highlights: http://www.gao.gov/highlights/d06371thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−371T

28. *April 04, Government Accountability Office* — **GAO−06−597T: Aviation Security: Transportation Security Administration Has Made Progress in Managing a Federal**

Security Workforce and Ensuring Security at U.S. Airports, but Challenges Remain (Testimony). It has been over three years since the Transportation Security Administration (TSA) assumed responsibility for passenger and baggage screening at commercial airports. This testimony focuses on the progress TSA is making in strengthening aspects of aviation security and the challenges that remain. Particularly, this testimony highlights (1) progress TSA has made, and challenges it faces, in managing a federalized security workforce −− including federal security directors and transportation security officers −− with operational responsibility for ensuring security of passengers and their baggage; and (2) actions TSA has taken, and the challenges it faces, to ensure appropriate regulatory oversight of other airport security activities. In prior reports, the Government Accountability Office (GAO) has made numerous recommendations designed to strengthen aviation security with respect to aviation workforce planning, deployment, and oversight. TSA generally agreed with GAO's recommendations and is taking actions to implement them. GAO also has ongoing reviews related to TSA staffing models and other aviation security issues, and may make additional recommendations as appropriate.
Highlights: http://www.gao.gov/highlights/d06597thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−597T

29. *April 03, Associated Press* — **Long−awaited O'Hare airport expansion begins.** After decades of debate and scrapped blueprints, crews are moving dirt and pouring concrete at Chicago's O'Hare International Airport for the largest airport expansion in the nation's history. The seven−year, $15 billion project is designed to eliminate most weather−related delays and erase O'Hare's reputation as the perennial knot in the nation's aviation system. "It should make the intolerable delays a thing of the past," said Joseph Schwieterman, a transportation expert at DePaul University. Much of O'Hare's problem can be traced to its pretzel−like runway configuration, which can make it tough to land planes in fog and wind. "That airfield has probably the most complex geometry of any airfield in the United States ... and possibly the planet," said Mary Rose Loney, a Miami aviation consultant who was Chicago's aviation commissioner in the late 1990s. Even in fair weather, the airport can be trouble. Since March 21, the Federal Aviation Administration has investigated three close calls on O'Hare's runways.
Source: http://www.usatoday.com/travel/flights/2006−04−03−ohare−expa nsion_x.htm

30. *April 03, Washington Post* — **MaxJet adds new British route.** Boutique airline MaxJet Airways launched its Dulles−to−Stansted, England, direct flight service on Monday, April 3, complete with beef tenderloin on demand, ample legroom, and almost fully reclining seats. It's an all business−class service, however, that, while far cheaper than premium seats in major airlines, will be well above most coach fares. From its fleet of attendants in triangle felt hats and pin−striped suits, to four−course meals including goat cheese salads and New York strip streaks, the Dulles−based company hopes to carve out a niche as other airlines are stripping down their in−flight service. The company's discount business−class service first launched in November 2005 with a route between John F. Kennedy airport and Stansted, a suburban London airport that has become a fast−growing hub for European discount airlines. Industry watchers have mixed opinions on the company's low−cost luxury strategy, yet MaxJet said it is planning more routes. Chief executive, Gary Rogliano said he expects the company to start producing a profit by early summer.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/02/AR2006040200722.html

[Return to top]

Postal and Shipping Sector

31. *April 04, DMNews* — **Potter: Energy costs cause upcoming rate increase filing.** The U.S. Postal Service (USPS) cannot continue to absorb high fuel costs, Postmaster General John E. Potter said on Monday, April 3, and the agency plans to file its next rate case as soon as this month. Also, smaller, annual increases could begin in 2009, he said. Since the USPS raised rates in 2002, "fuel has risen more than $1 a gallon, costing the postal service over $1 billion a year for the gasoline we purchase directly," Potter said in his keynote speech at the 2006 National Postal Forum held April 2−5, in Orlando, FL. In addition, the USPS has never added a fuel surcharge, he said, absorbing all of the costs. Healthcare is another cost driver for the USPS. The filing with the Postal Rate Commission could come as soon as this month, he said. Insiders here expect it April 17, with implementation next spring. The agency plans to move toward smaller, annual increases beginning in 2009, Potter said. Potter also discussed intelligent mail and the four−state barcode. "Without cluttering up the envelope, the new codes will provide a rich source of data to manage mail, track performance and create value," he said.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=3633 4

32. *April 04, Government Computer News* — **USPS orders more wireless asset management systems.** The U.S. Postal Service (USPS) is expanding its use of asset management systems that help track the agency's industrial power vehicles. USPS has ordered the Wireless Asset Net management system for 16 locations, bringing the total number of agency facilities to 38. Consisting of wireless devices installed on industrial vehicles such as forklifts and pallet movers, the Wireless Asset Net helps organizations track and maintain the location and status of such vehicles. The system also restricts vehicle access to trained, authorized operators and provides electronic safety inspection checklists.
Source: http://www.gcn.com/online/vol1_no1/40314−1.html

[Return to top]

Agriculture Sector

Nothing to report.
[Return to top]

Food Sector

33. *April 04, Agence France−Presse* — **Half of Japan's safety panel on U.S. beef resigns.** Half of the 12−member research panel on the safety of U.S. beef has resigned, an official said, amid growing pressure on Tokyo to resume imports stopped twice over fears of mad cow disease. The six members resigned after expressing caution about immediately resuming beef imports from the U.S., Jiji Press and Kyodo News reported. The research panel of the Food Safety Commission has already appointed new members to replace the six.
Source: http://www.cattlenetwork.com/content.asp?contentid=27234

[Return to top]

Water Sector

34. *April 04, Herald Tribune (FL)* — **Polluted ground water leaks at Piney Point.** Ground water containing ammonia levels 15 times higher than normal leaked from an abandoned phosphate mine at Piney Point, FL, onto a nearby farm in December and January. Florida Department of Environmental Protection (DEP) officials say the polluted area, some 300 feet from the mine, was limited to a Florida Power & Light easement on the farm and that no harm was done to crops. But the seepage is another black mark against the mine that has had pollution problems since owner Mulberry Corp. went bust, leaving the DEP to clean up the mess. The DEP has spent more than $80 million cleaning up Piney Point. It is expected to cost an additional $40 million.
Source: http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/20060404/NEWS/604040495/1006/SPORTS

35. *April 03, South Florida Business Journal* — **Backup generators to keep water flowing in West Palm Beach.** West Palm Beach, FL, workers are installing two massive backup power generators designed to make the power supply at the city's water treatment plant more hurricane resistant. The city said the installation is part of its proactive approach to help keep residents safe during what is forecast to be a busy 2006 hurricane season. When activated, the city said generators supply 2,000 kilowatts of power each, enabling the water treatment plant to run at full capacity at all times.
Source: http://www.bizjournals.com/southflorida/stories/2006/04/03/daily4.html?from_rss=1

[Return to top]

Public Health Sector

36. *April 04, Prime−Tass (Russia)* — **Russia manages to contain avian flu in four regions.** Russian veterinarians have managed to eradicate the H5N1 strain of avian flu in six Russian regions and the infection remains registered in four other regions, Russia’s Federal Service for Veterinarian and Phytosanitarian control said Tuesday, April 4. There are 15 villages and towns still affected by the disease, while the situation has been normalized in 52 villages and towns during the past three months, the service said. Of the areas where the disease still needs to be dealt with, the largest number are located in South Russia’s Krasnodar Region. Other affected areas are situated in neighboring Stavropol Region, as well as in the constituent republic of Dagestan in North Caucasus and the Volgograd Region.
Source: http://www.prime−tass.com/news/show.asp?topicid=68&id=394965

37. *April 04, Agence France−Presse* — **Indonesia records 24th bird flu death.** An eight−year−old Indonesian girl who died last year has been confirmed by the World Health Organization (WHO) as the nation's 24th bird flu fatality, a health ministry official said. Runizar Rusin, the head of the ministry's bird flu command post, said that samples taken from the girl were only recently sent to Hong Kong for testing by a WHO−affiliated laboratory.

Source: http://news.yahoo.com/s/afp/20060404/wl_asia_afp/healthfluindonesia_060404105807;_ylt=Aty5fjH4zBKbEZ6uvmFzvI2JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

38. *April 04, BBC News* — **Burkina Faso confirms bird flu.** Burkina Faso has become the fifth African country to confirm an outbreak of the H5N1 strain of bird flu. Minister for Animal Resources Tiemoko Konate said the disease had been found in samples taken from a farm near the capital, Ouagadougou. A total of 65 samples from different regions had been sent for analysis to a laboratory in Italy, Konate said. Earlier this year Nigeria, Cameroon, Niger and Egypt reported their first cases of the deadly strain.
Source: http://news.bbc.co.uk/2/hi/africa/4875032.stm

39. *April 03, Los Alamos National Laboratory* — **Avian flu modeled on supercomputer, explores vaccine and isolation options for thwarting a pandemic.** Using supercomputers to respond to a potential national health emergency, scientists have developed a simulation model that makes predictions about the possible future course of an avian influenza pandemic. The large−scale, stochastic simulation model examines the nationwide spread of a pandemic influenza virus strain should it become transmissible human−to−human. The simulation rolls out a city− and census−tract−level picture of the spread of infection through a synthetic population of 281 million people over the course of 180 days, and examines the impact of interventions, from antiviral therapy to school closures and travel restrictions, as the vaccine industry struggles to catch up with the evolving virus. “Based on the present work ... we believe that a large stockpile of avian influenza−based vaccine containing potential pandemic influenza antigens, coupled with the capacity to rapidly make a better−matched vaccine based on human strains, would be the best strategy to mitigate pandemic influenza,” said the researchers. “It's probably not going to be practical to contain a potential pandemic by merely trying to limit contact between people (such as by travel restrictions, quarantine or even closing schools), but we find that these measures are useful in buying time to produce and distribute sufficient quantities of vaccine and antiviral drugs,” said researchers.
Source: http://www.lanl.gov/news/index.php?fuseaction=home.story&sto ry_id=8171

[Return to top]

Government Sector

40. *April 04, CBS/Associated Press* — **Capitol evacuated after power outage.** Police ordered an evacuation of the U.S. Capitol shortly after noon Monday, April 3, after the building lost power. The lights went back on less than an hour later, utility officials said. Electricity was restored about half an hour later, but officials decided to keep the building evacuated until the cause of the outage was determined, said Bob Stevenson, a spokesperson for Senate Majority Leader Bill Frist, R−TN. Mary−Beth Hutchinson, a spokesperson for Potomac Electric Power Co., said the electricity was shut off automatically after there was "a momentary drop in voltage due to customer operations up the lines" away from the Capitol. A Department of Homeland Security official said it was a "simple power outage" that affected only the Capitol and not any nearby office buildings. Before the evacuation sirens went off, more than 100 visitors sat in the darkened House gallery. They exited with everyone else when the alarm sounded, calmly walking toward exits.

Source: http://www.cbsnews.com/stories/2006/04/03/national/main14645 90.shtml

[Return to top]

Emergency Services Sector

41. *April 04, Houston Chronicle* — **National Hurricane Conference's expected attendance reflects widespread worry of upcoming hurricane season.** Still reeling from 2005's overwhelming hurricane blasts, emergency managers at all levels of government worry openly at what could happen when the new hurricane season begins June 1. Federal, state and local officials are grasping for ways to reassure the public that government can save lives through efficient evacuations and provide help quickly if the country experiences another destructive season. Expected attendance at the 28th Annual National Hurricane Conference in Orlando, FL, being held Monday though Friday, April 10−14, reflects public officials' intense concerns about hurricane threats that have swept the nation in recent years. Keynote speakers include Homeland Security Secretary Michael Chertoff and Acting Federal Emergency Management Agency Director R. David Paulison. Jack Colley, director of the Texas Division of Emergency Management, is also scheduled as a keynote speaker at the conference. He said he will tell participants that his agency, the transportation department, and local officials have worked out problems that created last year's deadly traffic fiasco, with which most of the 137 Hurricane Rita−related deaths were connected. Texas officials now are confident they can safely and quickly move hundreds of thousands of people out of coastal storm surge zones this year, if necessary, Colley said.
Source: http://www.chron.com/disp/story.mpl/metropolitan/3768834.htm l

42. *April 03, Texas Engineering Extension Service* — **Urban search and rescue robots nationwide deploy for evaluation exercise.** Ground, aerial and aquatic emergency response robots from across the country will face realistic urban search and rescue challenges Tuesday through Friday, April 4−7, at Disaster City near the Texas A&M University campus in College Station, TX. The event, hosted by Texas A&M Engineering and the Federal Emergency Management Agency Urban Search and Rescue Team Texas Task Force 1, is the second in a series of robot evaluation exercises for urban search and rescue applications conducted by the Department of Commerce's National Institute of Standards and Technology. The program is sponsored by the Department of Homeland Security's Science and Technology Directorate.
Source: http://www.teex.com/teex.cfm?pageid=teexresc&area=teex&story id=545&templateid=23

43. *April 03, Tennessean* — **"Dead spots" create emergency situation.** Bill Jorgensen, director of Williamson County, TN's, Department of Emergency Communications, has asked for $1.3 million to fix the problem of "dead spots" −− places where deputies, ambulance drivers and firefighters can't get a radio signal. He wants the county to put up more radio towers, boosting the strength and broadening the coverage of the county's public safety frequencies. Officials from the Sheriff's Office, volunteer fire departments and Williamson Medical Center say the "dead spots" have been around for more than 20 years. There have been many occasions when deputies needed to call for backup, but couldn't because the portable radios they carry on their belts couldn't pick up a signal. Sgt. Mark Elrod, who supervises the evening patrol shift at the Sheriff's Office, said he's also heard dispatchers call deputies who were unable to respond

because their radios couldn't get a signal. Jorgensen said a system of four, 180−foot−tall radio towers spread across the county will solve the problem.
Source: http://tennessean.com/apps/pbcs.dll/article?AID=/20060403/COUNTY090101/604030312

44. *April 03, WTHR (IN)* — **Radio failure impairs storm response in Indiana.** In the midst of severe weather which included severe thunderstorms and tornado warnings for the Indianapolis area, the public safety radio communication system failed. The 90−minute failure cut communications between local dispatchers and emergency responders when a limb fell on a power line, causing the generator to kick on. This, in turn, caused the communication system to shut down and internally reboot over and over again. As a result, all 33 dispatchers and controllers on duty had to resort to an old standby −− portable radios. This is not the first time the outdated 15−year old system has failed in time of crisis. The Metropolitan Emergency Communications Agency will soon enter into negotiations for a new digital radio system.
Source: http://www.wthr.com/Global/story.asp?S=4721121

45. *April 02, Mohave Daily News (AZ)* — **New software to store emergency response plans online.** Clark County, NV, casinos now have an improved system to develop and implement emergency response plans as required by Nevada law. Utilizing a software database program known as City Watch, developed by Las Vegas Metropolitan Police Department's Homeland Security Bureau, casinos, public utilities, public transit systems and ancillary businesses would be able to store their plans securely on the Internet. The law was enacted in 2003. It requires casinos and other properties that could be subject to a crisis situation to file emergency response plans with the state. The law, Nevada Revised Statutes 463.790, requires resorts to maintain the plans and was designed to let first responders know how individual properties would react in the event of a terrorist attack or other disaster. The program was funded by a federal Homeland Security grant. Homeland Security Bureau Sgt. Kim Veillon said if the Clark County program is successful, Governor Kenny Guinn may implement it statewide.
Source: http://www.mohavedailynews.com/articles/2006/04/03/news/top_story/top1.txt

[Return to top]

Information Technology and Telecommunications Sector

46. *April 03, Security Focus* — **MySQL query logging bypass vulnerability.** MySQL is susceptible to a query logging bypass vulnerability. This issue is due to a discrepancy between the handling of NULL bytes in input data. Analysis: This allows attackers to bypass the query logging functionality of the database so they can cause malicious SQL queries to be improperly logged. This may help them hide the traces of malicious activity from administrators. Vulnerable: MySQL AB MySQL 5.0.18; MandrakeSoft Linux Mandrake 2006.0 x86_64; MandrakeSoft Linux Mandrake 2006.0; MandrakeSoft Linux Mandrake 10.2 x86_64; MandrakeSoft Linux Mandrake 10.2; MandrakeSoft Corporate Server 3.0 x86_64; MandrakeSoft Corporate Server 3.0. Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/16850/references

47. *April 03, FrSIRT* — **IBM WebSphere Application Server remote denial−of−service vulnerability.** A vulnerability has been identified in IBM WebSphere Application Server, which could be exploited by attackers to cause a denial−of−service. Analysis: This flaw is due to an error when processing HTTP requests with overly large headers, which could be exploited by remote attackers to crash a vulnerable Web server, creating a denial−of−service condition. Affected products: IBM WebSphere Application Server version 4.0.1; IBM WebSphere Application Server version 4.0.2; IBM WebSphere Application Server version 4.0.3. Solution: Apply APAR PQ62144 or FixPack 4.0 (4.0.4): http://www.ibm.com/software/webservers/appserv/was/support/ Source: http://www.frsirt.com/english/advisories/2006/1214

48. *April 03, Network World* — **IEEE 802.11w fills wireless security holes.** IEEE 802.11i, the standard behind Wi−Fi Protected Access and WPA 2, patched the holes in the original Wired Equivalent Privacy specification by introducing new cryptographic algorithms to protect data traveling across a wireless network. Now, the 802.11w task group is looking at extending the protection beyond data to management frames, which perform the core operations of a network. Traditionally, management frames did not contain sensitive information and did not need protection. But with new fast handoff, radio resource measurement, discovery and wireless network management schemes, new and highly sensitive information about wireless networks is being exchanged in these non−secure frames. IEEE 802.11w proposes to extend 802.11i to cover these important frames. Source: http://www.networkworld.com/news/tech/2006/040306−80211w−wireless−security.html

49. *April 03, Federal Computer Week* — **Framework could aid global information exchange.** An open−standards group has created a framework that could facilitate the global exchange of information among organizations. The Open Group's Universal Data Element Framework (UDEF) has the potential to hasten information exchange by indexing the world's datasets in one universally shared semantic repository. And evidence shows that UDEF works. In October 2005, Open Group officials demonstrated the framework for members of the information technology community. The demonstration applied UDEF to a disaster response situation. In the scenario, an imaginary emergency response team wanted information about the availability of 9−volt batteries in a retailer's inventory database. An address repository managed by the U.S. Postal Service allowed the workers to determine the response team's location in relation to manufacturers and retailers. Access to Office Depot's database allowed the hypothetical workers to quickly check the batteries' inventory status. Finally, MapQuest let users plot driving routes to stores that had batteries available. Ron Schuldt, chairman of the Open Group UDEF Forum, said the framework's coding provides a semantic link among disparate datasets. "If the UDEF is adopted on a global scale, enterprises will be able to reduce the costs of building and maintaining interfaces between enterprise applications," said Schuldt. Source: http://fcw.com/article92807−04−03−06−Print

50. *March 31, ZDNet UK* — **Yahoo calls for effective cybercrime laws.** Yahoo on Thursday, March 30, called for "effective" legislation combined with industry self−regulation, to deal with online fraud, child abuse, and other cybercrime. The Internet services giant called on policy makers to concentrate on defining illegal use of technology, rather than how an action breaks the law. "The lack of global legislation adds to the complexity of the situation. It's not realistic

to have global legislation, but we do need international consistency," said Robin Pembrooke, director of product operations for Yahoo Europe. Pembrooke advocated a combination of legislation and self−regulation of Internet businesses in order to combat cybercrime. Source: http://news.zdnet.co.uk/internet/security/0,39020375,3926060 1,00.htm

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of an active exploitation of a cross site scripting vulnerability in the eBay website. Successful exploitation may either allow an attacker to obtain sensitive data from stored cookies or redirect auction viewers to phishing sites where further disclosure of login credentials or personal information can occur. For more information about the reported vulnerability can be found in the following:

CA−2000−02 CERT Advisory: Malicious HTML Tags Embedded in Client Web Requests http://www.cert.org/advisories/CA−2000−02.html

VU#808921 US−CERT Vulnerability Note: eBay contains a cross site scripting vulnerability http://www.kb.cert.org/vuls/id/808921

US−CERT recommends the following:

Disable Scripting as specified in the Securing Your Web Browser document at URL: http://www.us−cert.gov/reading_room/securing_browser/#how_to_secure

The Malicious Web Scripts FAQ information at URL:http://www.cert.org/tech_tips/malicious_code_FAQ.html#st eps

Validate web site addresses as described in the eBay Spoof Email Tutorial information at URL: http://www.microsoft.com/technet/security/advisory/917077.mspx

ST04−014 US−CERT Cyber Security Tip document at URL: http://www.us−cert.gov/cas/tips/ST04−014.html

ST05−010 Validate web site certificates as described in US−CERT Cyber Security Tip document at URL: http://www.us−cert.gov/cas/tips/ST05−010.html

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are

being targeted. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 27754 (−−−), 6881 (bittorrent), 25 (smtp), 3250 (−−−), 445 (microsoft−ds), 4142 (oidocsvc), 32768 (HackersParadise), 55620 (−−−), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

51. *April 04, Southwest Farm Press* — **Problems with Oklahoma's flood dams gain attention.** The recent rupture of an earthen dam in Hawaii was a warning to Oklahoma: It's time to focus on the rehabilitation of local flood control dams, according to Dan Lowrance, president of the Oklahoma Association of Conservation Districts in Oklahoma City. He continued, "Most Oklahomans fail to realize that our state has more flood control dams than any other state in the Union and that without repair it will be Oklahoma instead of Hawaii in the news." Lowrance said the state is looking at several ways to address this problem, including additional funding through the legislature. He said any funds appropriated by the state to rehabilitate these dams would be matched two−to−one by the federal government.
Source: http://southwestfarmpress.com/news/06−04−04−flood−dams−atten tion/

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer